CEQUENCE SECURITY

FIRST HALF 2022

API Protection Report

Shadow APIs and Automated Abuse Explode

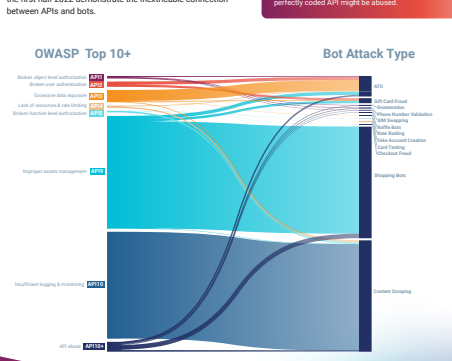
APIs are the heart of all things digital, and their ubiquitous use provides attackers with significant opportunities to discover exploitable coding errors or to use bots to attack perfectly coded APIs.

APIs and Bots: Inextricably Connected

Analysis of more than 20 billion transactions observed in the first half 2022 demonstrate the inextricable connection between APIs and bots.

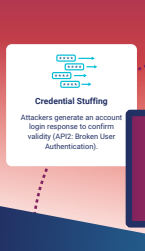
API Protection Tip

Look beyond the OWASP API Security Top Ten to a category defined as API10+: API Abuse that encompasses the different ways a perfectly coded API might be abused.



Shadow APIs are the #1 Attack Vector

Roughly **31%, or 5 billion of the 16.7 billion malicious transactions observed** targeted unknown, unmanaged and unprotected APIs.



Drivers

Insufficient visibility and inventory tracking (OWASP API9: Improper Asset Management), poor quality assurance, no formal publication process, internal APIs publicly exposed.

Abuse Examples

Sneaker Bots | Third-party Payment APIs | Credit and Gift Card Checking | Content Scraping

API10+: Perfectly Coded APIs Abused by Bots

API10+ highlights how attackers target perfectly coded and accurately inventoried APIs to achieve a wide range of end goals.

BLOCKED MALICIOUS REQUESTS

3 Billion
Shopping Bots

290 Million
Malicious Gift Card Checks

237 Million
Fake Account Requests

37 Million
Comment Spam Requests

API Protection Tip

Use API10+ to understand the connection between APIs and bots - an API only view would miss the behavioral abuse patterns that fall into this category.

ATO Mitigation Saves $193 Million

Often the result of Broken User Authentication (API2) errors, account takeovers remain popular due to their versatility, which is amplified by API adoption for account logins.

1.17 Billion
ATO Attempts Mitigated

11.7 Million
Accounts Protected

$290
Per Account Protected

$193 Million
Total Money Saved

Average 1% ATO success rate times the $290 cost per account (Juniper Research)

ATO Goals

From funds or loyalty points theft to fraud by executing a purchase or gift card validation from a compromised account.

Blocked Inventory API Attack Saves $80,000

Attackers leveraged OWASP API4 (Lack of Resources and Rate Limiting) and API5 (Broken Function Level Authorization) to enumerate a local inventory API used by Ulta Beauty.

Behaviors Observed

Rotated across 153,000 unique product and SKU combinations.

Scraped 61,000 ZIP codes and 33,000 products.

Results

$80,000 saved: 85.9 million malicious requests blocked resulting in infrastructure and loss prevention savings.

SIM Swapping and OWASP API1

Attackers tried to digitally steal mobile devices using Broken Object Level Authorization (API1) to:

1. Determine account transfer eligibility
2. Impersonate account owner to initiate SIM card transfer
3. Take control of the other accounts using SMS-based two factor authentication

9 Million +
malicious requests were mitigated based on behaviors observed

Behaviors Observed

High proxy IP address rotation

Perfect timing: A single request per IP every 2 seconds

High IP request ratio: Each API endpoint hit from over 200 IPs

Multiple OWASP Threats Used in Unison

The use of API2, API3, and API9 together signifies a high level of API analysis attackers are performing to achieve their end goal.

API Protection Tip

Developers and security teams alike must stay ever vigilant in following API coding and protection best practices.

Credential Stuffing

Attackers generate an account login response to confirm validity (API2: Broken User Authentication).

Sensitive Data Exposure

Attackers confirm their targets using data collected from API responses (API3 Excessive Data Exposure).

Shadow APIs

Attackers find APIs susceptible to API2 and API3 that were unknown and unprotected (API9 Improper Assets Management).

Partner Ecosystem APIs Enable Digital Supply Chain Attack

Attackers targeted a financial services partner ecosystem API to execute a series of coordinated credential stuffing attacks against multiple financial institutions:

50 Million +
malicious requests were mitigated based on behaviors observed

Behaviors Observed

Traffic from countries with no business dealings

Known malicious infrastructure

High session rotation

High login failure rate

Read the full API Protection Report, First Half 2022

Download Now

Continuous API Protection

The Cequence Unified API Protection (UAP) solution goes beyond API security approaches that may focus solely on one aspect of the API protection journey.

Schedule a personalized demo at **www.cequence.ai/demo/**

CEQUENCE SECURITY
100 S. Murphy Avenue, Suite 300, Sunnyvale, CA 94086 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai